Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended): A system for automatically protecting private video content using embedded cryptographic security, comprising:

a recorder frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

an encryption module encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium;

a decryption module retrieving encrypted frames from the transportable storage medium and decrypting each encrypted frame into decrypted frames using a decryption cryptographic key that is verified prior to decryption; [[and]]

a playback frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium; and

a verification module retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame, and comparing the verification cryptographic hash and the original cryptographic hash.

2. (canceled).

3. (currently amended): A system according to Claim [[2]] 1, further comprising:

an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

4. (original): A system according to Claim 1, further comprising:

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames.

5. (original): A system according to Claim 1, further comprising:

an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

6. (original): A system according to Claim 5, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

7. (original): A system according to Claim 1, further comprising:

a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

8. (original): A system according to Claim 1, further comprising:

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

9. (original): A system according to Claim 8, further comprising:

a set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key.

10. (currently amended): A method for automatically protecting private video content using embedded cryptographic security, comprising:

dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames on a transportable storage medium;

retrieving encrypted frames from the transportable storage medium and decrypting each encrypted frame into decrypted frames using a decryption cryptographic key that is verified prior to decryption; [[and]]

combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key; and

generating a verification fixed-length cryptographic hash from at least one such corresponding decrypted frame and comparing the verification cryptographic hash and the original cryptographic hash.

11. (canceled).

12. (currently amended): A method according to Claim [[11]] 10, further comprising:

providing an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

13. (original): A method according to Claim 10, further comprising:

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames.

14. (original): A method according to Claim 10, further comprising:

providing an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

15. (original): A method according to Claim 14, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

16. (original): A method according to Claim 10, further comprising:

providing a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

17. (original): A method according to Claim 10, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

18. (original): A method according to Claim 17, further comprising:

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium.

19. (currently amended): A computer-readable storage medium holding code for performing the method according to Claims 10, [[11,]] 12, 13, 14, 15, 16, 17, or 18.

20. (currently amended): A system for encrypting private video content using embedded cryptographic security, comprising:

a frame buffer receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

a processor encrypting each individual frame into encrypted video content using an encryption key selected from a cryptographic key pair; and

a recorder storing the encrypted frames on a transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair,

wherein the processor generates a fixed-length original cryptographic hash from at least one such individual frame and encrypts the original cryptographic hash using an encryption cryptographic key selected from the cryptographic key pair and the recorder stores the encrypted original cryptographic hash as a digital signature on the transportable storage medium for retrieval and verification using a decryption key selected from the cryptographic key pair.

21. (canceled).

22. (currently amended): A system according to Claim [[21]] 20, further comprising:

a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

23. (original): A system according to Claim 20, further comprising:
a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

24. (original): A system according to Claim 20, further comprising:
a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

25. (original): A system according to Claim 20, further comprising:
a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

26. (currently amended): A method for encrypting private video content using embedded cryptographic security, comprising:
receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;
encrypting each individual frame into encrypted video content using an encryption key selected from a cryptographic key pair; [[and]]
storing the encrypted frames on a transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair;
generating a fixed-length original cryptographic hash from at least one such individual frame;
encrypting the original cryptographic hash using an encryption cryptographic key selected from the cryptographic key pair; and
storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium for retrieval and verification using a decryption key selected from the cryptographic key pair.

27. (canceled).

28. (currently amended): A method according to Claim [[27]] 26, further comprising:

employing a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

29. (original): A method according to Claim 26, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

30. (original): A method according to Claim 26, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

31. (original): A method according to Claim 26, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

32. (currently amended): A computer-readable storage medium holding code for performing the method according to Claims 26, [[27,]] 28, 29, 30 or 31.

33. (currently amended): A system for decrypting private video content using embedded cryptographic security, comprising:

a player retrieving encrypted frames from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

a processor decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair; and

a frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form,

wherein the player retrieves a digital signature from the transportable storage medium, the digital signature containing an original cryptographic hash

encrypted using an encryption cryptographic key selected from the cryptographic key pair, and the processor decrypts the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair, generates a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium, and compares the verification cryptographic hash and the original cryptographic hash.

34. (canceled).

35. (currently amended): A system according to Claim [[34]] 33, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

36. (original): A system according to Claim 33, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

37. (original): A system according to Claim 33, further comprising:

a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

38. (original): A system according to Claim 33, further comprising:

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

39. (currently amended): A method for decrypting private video content using embedded cryptographic security, comprising:

retrieving encrypted frames from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair; [[and]]

combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form;

retrieving a digital signature from the transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from the cryptographic key pair;

decrypting the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair; and

generating a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium and comparing the verification cryptographic hash and the original cryptographic hash.

40. (canceled).

41. (currently amended): A method according to Claim [[40]] 39, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

42. (original): A method according to Claim 39, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

43. (original): A method according to Claim 39, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

44. (original): A method according to Claim 39, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

45. (currently amended): A computer-readable storage medium holding code for performing the method according to Claims 39, [[40,]] 41, 42, 43 or 44.

46. (currently amended): A system for automatically authenticating private video content using embedded cryptographic security, comprising:

a recorder frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

a signature module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key comprising a private key of an asymmetric cryptographic pair, and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

a verification module retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key comprising a public key of an asymmetric cryptographic pair; and

a player frame buffer generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash.

47. (canceled).

48. (currently amended): A system according to Claim [[47]] 46, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

49. (original): A system according to Claim 46, further comprising:

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

50. (original): A system according to Claim 49, further comprising:

a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key stored on the removable storage medium.

51. (currently amended): A method for automatically authenticating private video content using embedded cryptographic security, comprising:

dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form and generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key comprising a private key of an asymmetric cryptographic pair and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key comprising a public key of an asymmetric cryptographic pair and

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash.

52. (canceled).

53. (currently amended): A method according to Claim [[52]] 51, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

54. (original): A method according to Claim 51, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

55. (original): A method according to Claim 54, further comprising:

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium.

56. (currently amended): A computer-readable storage medium holding code for performing the method according to Claims 51, [[52,]] 54 or 55.

57. (original): A system for digitally signing private video content using embedded cryptographic security, comprising:

a frame buffer receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

a processor generating a fixed-length original cryptographic hash from at least one such individual frame and encrypting the original cryptographic hash using an encryption cryptographic key selected from a cryptographic key pair; and

a recorder storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and verification using a decryption key selected from the cryptographic key pair.

58. (original): A system according to Claim 57, further comprising:

a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

59. (original): A system according to Claim 57, further comprising:

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

60. (original): A method for digitally signing private video content using embedded cryptographic security, comprising:

receiving a substantially continuous video signal representing raw video content and dividing the data signal into individual frames which each store a fixed amount of data in digital form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key selected from a cryptographic key pair; and

storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and verification using a decryption key selected from the cryptographic key pair.

61. (original): A method according to Claim 60, further comprising:

employing a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

62. (original): A method according to Claim 60, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

63. (original): A computer-readable storage medium holding code for performing the method according to Claims 60, 61 or 62.

64. (original): A system for verifying digitally signed private video content using embedded cryptographic security, comprising:

a player retrieving a digital signature from a transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from a cryptographic key pair;

a processor decrypting the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair, generating a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium, and comparing the verification cryptographic hash and the original cryptographic hash.

65. (original): A system according to Claim 64, further comprising:
a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

66. (original): A system according to Claim 64, further comprising:
a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

67. (original): A method for verifying digitally signed private video content using embedded cryptographic security, comprising:
retrieving a digital signature from a transportable storage medium, the digital signature containing an original cryptographic hash encrypted using an encryption cryptographic key selected from a cryptographic key pair;
decrypting the encrypted original cryptographic hash using a decryption cryptographic key selected from the cryptographic key pair; and
generating a verification fixed-length cryptographic hash from at least one individual frame retrieved from the transportable storage medium and comparing the verification cryptographic hash and the original cryptographic hash.

68. (original): A method according to Claim 67, further comprising:
employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

69. (original): A method according to Claim 67, further comprising:
providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

70. (original): A computer-readable storage medium holding code for performing the method according to Claims 67, 68 or 69.